Claim Amendment under 37 C.F.R. §1.121

1.   (Currently amended)   An access control system, comprising:

a Virtual Secure Disk (VSD) image file module occupying a certain space of a hard disk in a file form;

a VSD drive for processing security-sensitive files within the VSD image file module;

an encryption and decryption module for encrypting and decrypting data input, output, or input and output input/output between the VSD image file module and the VSD drive;

a VSD file system module for allowing an operating system to recognize the VSD drive as a separate disk volume at a time of access to the security-sensitive files within the VSD image file module; and

an access control module for determining access by determining whether an access location is a disk drive or the VSD drive and an [[the]] application module has been authorized to access a certain file at a time of access to the file, which is stored on the hard disk, to perform tasks in the application module, wherein an authorized application module is configured to access the VSD drive for write and read operations, wherein the authorized application module is configured to access the disk drive for a read operation only, wherein an unauthorized application module is configured to access the disk drive for write and read operations, and wherein the unauthorized application module is not allowed to access the VSD drive.

2.   (Currently amended)   The access control system according to claim 1, wherein the access control module comprises:

an extended system service table for allowing the operation of a corresponding function to be performed when it is pointed at by a descriptor; and

an extended system table for changing a function, which is requested of the service system table by the application module, to prevent operation of the function, determining whether a space in which a corresponding task is performed is the disk drive or the VSD drive, determining whether access to the corresponding file by the application module has been authorized, and providing an [[the]] unchanged function to the extended system service table or stopping the operation of the function according to results of the determination.

3.   (Currently amended) The access control system according to claim 1 or 2, wherein the VSD image file module virtually occupies the hard disk so as to allow the operating system to recognize the data as being assigned to a certain space of the hard disk without performing physical assignment for storing the data on the hard disk, so that an [[the]] authorized application module can physically assign the data to the space.

4.   (Currently amended) An access control method, which is performed by an access control system having a hard disk, a disk drive, a file system module, an application module, a VSD image file module, a VSD drive, an encrypting and decrypting ~~encrypting/decrypting~~ module, a VSD file system module, and a control access module including an extended system service table and an extended service table, wherein the VSD image file module occupies a certain space of the hard disk in a file form and the VSD drive for processing security-sensitive files is located within the VSD image file module, the access control method comprising the steps of:

    (a) authorizing the application module ~~modules~~;

    (b) the application module calling a function from an operating system to access a corresponding file;

    (c) the operating system providing the function to the extended service table;

    (d) changing the function into an arbitrarily designated function to prevent the operation of the function in the extended service table;

    (e) determining whether an ~~the~~ access space of the file is the disk drive or the VSD drive in the extended service table;

    (f) returning the arbitrarily designated function to the original function whose operation is possible, and providing the original file to the extended system service table if it is determined that the access space is the disk drive at step (e);

    (g) determining whether ~~access to~~ the application module has been authorized if it is determined that the access space is the VSD drive ~~disk drive~~ at step (e);

    (h) returning the arbitrarily designated function to the original function whose operation is possible, and providing the original function to the extended system service table if it is determined that the application module has been authorized at step (g); and

(i) stopping the operation of the corresponding function if it is determined that the application module has not been authorized at step (g).

5.   (Currently amended)   The ~~application-based~~ access control method according to claim 4, wherein, if the function is a function requesting a Write operation, the step (e) comprises the steps of:

determining whether the application module has been authorized; stopping the operation of the function if it is determined the application module has been authorized; and

the arbitrarily designated function returning to the original function, the operation of which is possible, and being provided to the extended system service table if it is determined that the application module has been unauthorized.

6.   (Original)   The access control method according to claim 4 or 5, further comprising the step of the encryption and decryption module encrypting and decrypting data that are input and output between the VSD image file module and the VSD drive.